JOURNAL OF ALGEBRA 15, 408–416 (1970)

On a Problem of E. Artin

MARCEL HERZOG

Department of Mathematics, Tel-Aviv University, Tel-Aviv, Israel

Communicated by W. Feit

Received September 10, 1969

1. INTRODUCTION

Following his studies on the order of known types of simple finite groups, E. Artin asked in a letter to R. Brauer: what are the simple finite groups of an order $o(G)$ which is divisible by a prime $p > o(G)^{1/3}$? He conjectured that all such groups belong to the known (in 1958) types. Artin's conjecture was proved by R. Brauer and W. F. Reynolds in [1]. They showed that only the simple groups $PSL(2, p)$ where $p > 3$ and $PSL(2, p-1)$, where $p > 3$ is a Fermat prime, satisfy Artin's condition.

In this paper a finite group with a cyclic Sylow p-subgroup P of order p^a will be called a Cp^a-group. In [5] the author classified all perfect Cp^a-groups G subject to the following two conditions:

$$o(G) < o(P)^3$$

and the Sylow p-subgroups of G constitute a (TI) set. Under these conditions the above mentioned list of groups is extended to contain $SL(2, p)$, where $p > 3$ is a prime, and $PSL(2, 8)$.

The object of this paper is to classify all non-p-solvable Cp^a-groups G subject to the single condition

$$o(G) < o(P)^3.$$

As a matter of fact, we will prove the following apparently more general result:

THEOREM 1. *Let G be a Cp^a-group and suppose that*

$$o(G) < p^{3a}$$

and no homomorphic image of G is isomorphic to $N_G(P)/W$, where W is the normal complement of P in $C_G(P)$. Then one of the following statements holds.

(I) $a = 1$, $G \simeq PSL(2, p)$, *where* $p > 3$ *is a prime.*

(II) $a = 1$, $G \simeq PSL(2, p - 1)$, *where* $p = 2^m + 1 > 5$ *is a Fermat prime.*

(III) $a = 1$, $G \simeq SL(2, p)$, *where* $p > 3$ *is a prime*

(IV) $a = 2$, $p = 3$, $G \simeq PSL(2, 8)$.

(V) $a = 1$, $G \simeq PGL(2, p)$, *where* $p > 3$ *is a prime.*

(VI) $a = 1$, $G \simeq PSL(2, p) \times M$, *where* $p > 3$ *is a prime and* $o(M) = 2$.

Theorem 1 follows quite easily from the following more special

THEOREM 2. *Let G be a perfect Cp^a-group and suppose that*

$$o(G) < p^{3a}.$$

Then one of the following statements holds.

(I) $a = 1$, $G \simeq PSL(2, p)$, *where* $p > 3$ *is a prime.*

(II) $a = 1$, $G \simeq PSL(2, p - 1)$, *where* $p = 2^m + 1 > 5$ *is a Fermat prime.*

(III) $a = 1$, $G \simeq SL(2, p)$, *where* $p > 3$ *is a prime.*

(IV) $a = 2$, $p = 3$, $G \simeq PSL(2, 8)$.

Theorem 2 follows, in turn, from Theorem 1 in [5] and the following reduction theorem.

THEOREM 3. *Let G be a perfect Cp^a-group and suppose that*

$$o(G) < p^{3a}.$$

Then the Sylow p-subgroups of G constitute a (TI) set.

Section 2 of this paper deals with some elementary properties of Cp^a groups which are of independent interest. Theorem 3 is proved in Section 3. The final Section 4 contains the proofs of Theorems 1 and 2.

We use the standard notation $C_G(T), N_G(T), o(T)$ and $T^{\#}$, where T is a subset of the group G, to denote respectively: the centralizer, normalizer, number of elements and the nonunit elements of T. We will say that $N_G(T)/C_G(T)$ acts frobeniusly on T if $\theta^{\eta} = \theta$ for $\theta \in T^{\#}$ and $\eta \in N_G(T)$ implies that $\eta \in C_G(T)$. An element of G is called a p'-element, where p is a prime number, if p does not divide its order. The principal character and the commutator subgroup of G will be denoted by 1_G and G' respectively. The i-th commutator subgroup of G will be denoted by $G^{(i)}$. Finally, if a and b are integers, then (a, b) denotes their greatest common divisor and $a \mid b$ means: a divides b.

2. Cp^a-Groups

In this section we will prove some elementary properties of groups mentioned in the title.

Proposition 2.1. *Let G be a Cp^a-group. Then:*

$$\begin{aligned} P \cap G' &= \{1\} && \text{if} \quad N_G(P) = C_G(P) \\ &= P && \text{if} \quad N_G(P) \neq C_G(P). \end{aligned}$$

Proof. If $N(P) = C(P)$, then $P \cap G' = \{1\}$ by [6, Theorem 6.2.10].

Otherwise $N_G(P)/C_G(P)$ acts frobeniusly on P [4, Lemma 2.1] and consequently $Z(N_G(P)) \cap P = \{1\}$. It follows then, from transfer theorems [6, pp. 393–5], that

$$P/P \cap G' \cong P \cap Z(N_G(P)) = \{1\}$$

and consequently $P \subset G'$.

Proposition 2.2. *Let G be a Cp^a-group. Then G is p-solvable if and only if G has a homomorphic image which is isomorphic to $N_G(P)/W$, where W is the normal complement of P in $C_G(P)$.*

Proof. Suppose first that there exists a normal subgroup K of G such that $G/K \cong N_G(P)/W$. Since $N_G(P)/W$ is solvable it follows that G is p-solvable.

If, on the other hand, G is p-solvable, then by Theorem 6.3.3 of [3] $P \subset 0_{p',p}(G) = H$ and $C_G(P) \subset H$. It follows that $H = KP$, where $K \lhd H$ and $K \cap P = \{1\}$. Since P is Abelian, $C_G(P) = P \times W$ and consequently $W = C_G(P) \cap K$. The group H possesses a normal p-complement K which implies, by a theorem of Frobenius [3, Theorem 7.4.5], that

$$N_H(P) = C_H(P) = C_G(P).$$

Since $H \lhd G$, we have

$$G = N_G(P)\, H = N_G(P)\, K$$

and

$$N_G(P) \cap K = N_H(P) \cap K = C_G(P) \cap K = W.$$

Thus:

$$\frac{G}{K} \cong \frac{N_G(P)}{N_G(P) \cap K} = \frac{N_G(P)}{W}$$

as required.

3. Proof of Theorem 3

Let $q = [N_G(P) : C_G(P)]$; then it is well-known that $1 \leqslant q \leqslant p - 1$ and $q \mid p - 1$ [4, Lemma 2.1]. Since G is perfect, P has no normal complement in G and consequently $q > 1$, $p > 2$.

It follows from [4, Proposition 2.1 and Corollary 2.1], taking into account the assumption $G = G'$, that the principal p block B of G contains q non-exceptional characters which can be written as follows:

$$\begin{array}{lll} R_0 = 1_G & R_0(\sigma) = 1, & R_0(1) = 1 \\ R_i(i = 1,\ldots, u) & R_i(\sigma) = 1, & R_i(1) = r_i p^a + 1 \\ S_i(i = 1,\ldots, v) & S_i(\sigma) = -1, & S_i(1) = s_i p^a - 1 \end{array}$$

where σ is any element of $P^{\#}$, s_i, r_i are positive integers, $o(P) = p^a$ and

$$u + v = q - 1. \tag{1}$$

The block B contains also $(p^a - 1)/q$ exceptional characters of degree $x_0 = bp^a - \epsilon_0 q$, where $\epsilon_0 = \pm 1$ and b is a nonnegative integer. In addition, the following relation holds:

$$0 = \sum_{i=0}^{u} R_i(1) - \sum_{i=1}^{v} S_i(1) + \epsilon_0(bp^a - \epsilon_0 q).$$

Consequently:

$$0 = \left(\sum_{i=1}^{u} r_i - \sum_{i=1}^{v} s_i + \epsilon_0 b \right) p^a + u + 1 + v - q$$

and in view of (1) we get:

$$\sum_{i=1}^{v} s_i = \sum_{i=1}^{u} r_i + \epsilon_0 b. \tag{2}$$

Since for $a = 1$ the theorem trivially holds, we will assume from now on that $a \geqslant 2$.

We proceed with 3 lemmas dealing with all the possible arrangements of the degrees $R_i(1)$, $i = 1,\ldots, u$ and $S_i(1)$, $i = 1,\ldots, v$ in B. A subgroup H of G will be called a CC-subgroup if H contains the centralizer of each of its nonunit elements.

Lemma 3.1. *Suppose that there exist in B two nonprincipal nonexceptional characters Y and Z of degrees $yp^a + \epsilon_1$ and $zp^a + \epsilon_2$ respectively, where $\epsilon_i = \pm 1$, $i = 1, 2$, and such that*:

$$yp^a + \epsilon_1 \neq zp^a + \epsilon_2, \qquad yz > 1. \tag{3}$$

Then P is a CC-subgroup of G. Consequently, Theorem 3 holds in this case.

Proof. Let $d = (yp^a + \epsilon_1, zp^a + \epsilon_2)$; then $d \mid (zyp^a + \epsilon_1 z, yzp^a + \epsilon_2 y)$ and consequently $d \mid |y - \epsilon_1\epsilon_2 z|$. As by (3) $y - \epsilon_1\epsilon_2 z \neq 0$, it follows that $d = |y - \epsilon_1\epsilon_2 z|/x$ where x is an integer. Since

$$p^a, yp^a + \epsilon_1, zp^a + \epsilon_2 \mid o(G)$$

it follows that

$$\frac{x(yp^a + \epsilon_1)(zp^a + \epsilon_2)p^a}{|y - \epsilon_1\epsilon_2 z|} \Bigg| \, o(G). \tag{4}$$

Suppose that either $x > 1$ or $x = 1$ and the division in (4) is proper. Then:

$$p^{3a} > o(G) \geqslant 2(yp^a - 1)(zp^a - 1)\, p^a/(y + z)$$

which yields

$$(y + z)\, p^a > 2yzp^a - 2y - 2z.$$

As $p^a > 8$, we have:

$$5(y + z)/4 > 2yz$$

in contradiction to the assumption $yz > 1$.

It follows that

$$o(G) = (yp^a + \epsilon_1)(zp^a + \epsilon_2)\, p^a/d$$

and consequently if r^e is the r-share in $o(G)$ of a prime $r \neq p$, then either $r^e \mid yp^a + \epsilon_1$ or $r^e \mid zp^a + \epsilon_2$. It follows by [2, Theorem 86.3] that if $\gamma \in G$ is not a p-element then:

$$\text{either} \qquad Y(\gamma) = 0 \qquad \text{or} \qquad Z(\gamma) = 0. \tag{5}$$

Let $\sigma \in P^{\#}$ and π be a p'-element of $C_G(\sigma)$. Then by [4, Proposition 2.1]

$$Y(\sigma\pi) = \epsilon_1, \qquad Z(\sigma\pi) = \epsilon_2$$

and it follows from (5) that $\sigma\pi$ is a p element, $\pi = 1$. Thus for all $\sigma \in P^{\#}$ we have $C_G(\sigma) = P$, as required. The (TI) property follows immediately.

LEMMA 3.2. *Suppose that the nonprincipal nonexceptional characters of B are all of the same degree $yp^a + \epsilon$. Then the conclusions of Lemma* 3.1 *hold.*

Proof. Since either $\epsilon = 1$, $u = q - 1$ or $\epsilon = -1$, $v = q - 1$, it follows from (2) that

$$y(q - 1) = b, \qquad \epsilon_0 = -\epsilon.$$

Thus,

$$x_0 = bp^a - \epsilon_0 q = q(yp^a + \epsilon) - yp^a$$

yielding $(x_0, yp^a + \epsilon) = 1$ and as $x_0, yp^a + \epsilon, p^a \mid o(G)$ we get

$$(y(q - 1)\, p^a + \epsilon q)(yp^a + \epsilon)\, p^a \mid o(G).$$

Suppose that at least one of the following cases holds: (i) $y > 1$; (ii) $q > 2$; (iii) the above division is proper. Then:

$$p^{3a} > o(G) \geqslant (2p^a - 4)(p^a - 1)\, p^a$$

which is impossible since $p^a > 6$. Therefore none of the cases (i)–(iii) holds and consequently

$$o(G) = (p^a + 2\epsilon)(p^a + \epsilon)\, p^a, \qquad q = 2.$$

Let Y denote the nonexceptional character of B of degree $p^a + \epsilon$ and let X be an exceptional character of B of degree $x_0 = p^a + 2\epsilon$. Since $(p^a + 2\epsilon, p^a + \epsilon) = 1$, the arguments used in Lemma 3.1 show that if $\sigma \in P^{\#}$ and π is a p' element of $C_G(\sigma)^{\#}$, then either $Y(\sigma\pi) = 0$ or $X(\sigma\pi) = 0$. However, it follows from [4, Proposition 2.1] that

$$Y(\sigma\pi) = \epsilon \qquad \text{and} \qquad X(\sigma\pi) = \epsilon(\lambda^{\tau_1}(\sigma) + \lambda^{\tau_2}(\sigma))$$

where λ is an irreducible character of P and $\{\tau_1, \tau_2\}$ is a set of coset representatives of $C_G(P)$ in $N_G(P)$. Obviously $Y(\sigma\pi) = 0$ is impossible and if $X(\sigma\pi) = 0$, then

$$\lambda^{\tau_1}(\sigma) = -\lambda^{\tau_2}(\sigma);$$

a contradiction to the fact that $\lambda^{\tau_1}(\sigma)$ and $\lambda^{\tau_2}(\sigma)$ are p^a-th roots of unity Consequently, if $\sigma \in P^{\#}$, then $C_G(\sigma)$ contains no p'-elements other than 1 and $C_G(\sigma) = P$. Thus P is a CC-subgroup of G. The (TI) property follows, and the proof of Lemma 3.2 is complete.

LEMMA 3.3. *Suppose that $u \neq 0$ and $v \neq 0$. Assume also that*

$$r_i = 1(i = 1,..., u) \qquad \textit{and} \qquad s_i = 1(i = 1,..., v).$$

Then the conclusions of Lemma 3.1 *hold.*

Proof. The block B contains nonexceptional characters of degrees $p^a - 1$ and $p^a + 1$. Consequently

$$(p^a - 1)(p^a + 1)\, p^a/2 \mid o(G).$$

If $o(G) = (p^a - 1)(p^a + 1)\, p^a/2$ then P is a CC-subgroup of G by the same arguments as used in Lemma 3.1. Thus it suffices to assume that the above division relation is proper and to derive a contradiction.

Since $p^a > 2$ and $o(G) < p^{3a}$, it follows from our assumptions that

$$o(G) = (p^a - 1)(p^a + 1)\, p^a.$$

As $r_i = s_j = 1$ for all i and j, Eqs. (1) and (2) yield:

$$\begin{aligned} v &= u + \epsilon_0 b \\ v + u &= q - 1. \end{aligned} \tag{6}$$

Assume first that $C(P) = P$. Then

$$o(G) = qp^a(np + 1) = (p^a - 1)(p^a + 1)\, p^a$$

and consequently $q \equiv -1 (\operatorname{mod} p)$. As $q \mid p - 1$, we get $q = p - 1$ and $b = \epsilon_0(v - u)$. Hence, $x_0 = bp^a - \epsilon_0 q = \epsilon_0[(v - u)\, p^a - (p - 1)]$ and as $v + u = p - 2$, $u \neq v$. We also have

$$(x_0 \,, p^a \pm 1) \mid p - 1 \pm (v - u).$$

Since $x_0 \mid o(G)$ and $(x_0 \,, p^a) = 1$ we get:

$$\begin{aligned} x_0 &\leqslant [p - 1 + (v - u)][p - 1 - (v - u)] \\ &= (p - 1)^2 - (v - u)^2 \leqslant (p - 1)^2. \end{aligned}$$

Therefore,

$$p^a - (p - 1) \leqslant x_0 \leqslant (p - 1)^2, \qquad p^a \leqslant p(p - 1)$$

in contradiction to our assumption that $a \geqslant 2$.

Thus it remains only to deal with the case $w = [C_G(P) : P] > 1$. Let X be the character S_1, then by [4, Proposition 2.1]

$$X(1) = p^a - 1 \qquad \text{and} \qquad X(\sigma\pi) = -1$$

for $\sigma \in P^{\#}$ and $\pi \in W$, where $C = C_G(P) = P \times W$. Denote the restriction of X to C also by X, then X is a character of $P \times W$ and therefore for $\rho \in P$ and $\pi \in W$ we have:

$$X(\rho\pi) = \sum_{i=1}^{r} \psi_i(\pi)\, \phi_i(\rho) \tag{7}$$

where ψ_i, $i = 1,..., r$ are distinct irreducible characters of W and ϕ_i, $i = 1,..., r$ are characters of P. Let $\sigma \in P^{\#}$, $\pi \in W$; as $X(\sigma\pi) = 1$, it follows from (7) and from the linear independence of the irreducible characters of W, that the principal character appears among the ψ_i, say $\psi_1 = 1_W$, and

$$\phi_1(\sigma) = -1, \qquad \phi_2(\sigma) = \cdots = \phi_r(\sigma) = 0.$$

Suppose that $r > 1$. Then ϕ_2 vanishes on $P^{\#}$ and therefore p^a divides $\phi_2(1)$, in contradiction to (7) and the fact that $X(1) = p^a - 1$. Thus $r = 1$ and

$$X(\rho\pi) = \phi_1(\rho) \qquad \text{for all} \quad \rho \in P, \quad \pi \in W.$$

In particular $X(\pi) = \phi_1(1) = X(1)$ for all $\pi \in W$. Let V denote the kernel of X, then V is a normal subgroup of G and $W \subset V$.

Let $o(V) = t$; as $W \subset V$, $t \geqslant 2$. Obviously $P \cap V = \{1\}$ and $G/V = L$ is a perfect Cp^a-group. We also have

$$o(L) < p^{3a}/t \leqslant p^{3a}/2. \tag{8}$$

It is easy to see that any perfect Cp^a-group has to satisfy the assumptions of one of the Lemmas 3.1, 3.2, or 3.3. In particular, L satisfies one of them, and in addition it satisfies the inequality (8). Thus by Lemmas 3.1, 3.2, and the first part of Lemma 3.3 the Sylow p-subgroups of L satisfy the (TI) property. As $a \geqslant 2$, it follows from Theorem 1 in [5] that $a = 2, p = 3$, and $L \cong PSL(2, 8)$ in contradiction to (8). The proof of Lemma 3.3 is complete.

As mentioned above, G has to satisfy the assumptions of one of the Lemmas 3.1, 3.2, or 3.3. Consequently, the Sylow p-subgroups of G constitute a (TI) set. The proof of Theorem 3 is complete.

4. Proof of Theorems 1 and 2

We begin with the proof of Theorem 2. It follows from Theorem 3 that the Sylow p-subgroups of G constitute a (TI) set. Consequently, by Theorem 1 of [5] one of the statements (I)–(IV) holds.

The proof of Theorem 1 is a little bit more complicated. If $a = 1$, then by Theorem 1* of [5] one of the statements (I), (II), (III), (V), or (VI) holds. If G is perfect, then by Theorem 2 one of the statements (I)–(IV) holds. Thus it suffices to assume that $a \geqslant 2$ and $G' \neq G$ and to derive a contradiction.

It follows from Proposition 2.2 that G is not p-solvable. Let $G^{(k)}$ be the first derived group of G satisfying $G^{(k)} = G^{(k-1)}$. Suppose first that $G^{(k)}$ does not contain P. Then by Proposition 2.1 there exists an integer i such that

$$P \subset G^{(i)}, \qquad C_{G^{(i)}}(P) = N_{G^{(i)}}(P) \qquad \text{and} \qquad 0 \leqslant i < k.$$

Hence by the Burnside Theorem

$$G^{(i)} = KP, \qquad K \lhd G^{(i)}, \qquad K \cap P = \{1\}.$$

But then

$$G \rhd G^{(i)} \rhd K \rhd \{1\}$$

is a normal series, in contradiction to the non-p-solvability of G. Consequently $P \subset G^{(k)}$. It follows then by Theorem 2 that $G^{(k)}$ is of one of the types (I)–(IV). As $a \geqslant 2$, we must have

$$a = 2, \qquad p = 3, \qquad \text{and} \qquad G^{(k)} \cong PSL(2, 8).$$

However, $o(G^{(k)}) \leqslant o(G)/2 < p^{3a}/2$, a contradiction. The proof of Theorem 1 is complete.

REFERENCES

1. R. BRAUER AND W. F. REYNOLDS, On a problem of E. Artin, *Ann. Math.* **68** (1958), 713–720.
2. C. W. CURTIS AND I. REINER, "Representation Theory of Finite Groups and Associative Algebras," Wiley (Interscience), New York, 1962.
3. D. GORENSTEIN, "Finite Groups," Harper and Row, New York, 1968.
4. M. HERZOG, On finite groups with cyclic Sylow subgroups for all odd primes, *Isr. J. Math.* **6** (1968), 206–216.
5. M. HERZOG, On finite groups with independent cyclic Sylow subgroups, *Pacific J. Math.* **29** (1969), 285–293.
6. W. R. SCOTT, "Group Theory," Prentice-Hall, Englewood cliffs, N. J., 1964.